COT Security Alert – SQL Injection Attacks

Targeted web application attacks, including SQL Injection attacks, are increasing on both government and private networks. A successful attack using SQL Injection may allow malicious entities access to sensitive data on the targeted system or give them the ability to attack website visitors with malicious content.

SQL Injection vulnerabilities exist in web applications where malicious user input is used to access the database without proper validation. Developers can prevent exploitation of these vulnerabilities by not allowing client-supplied data to modify SQL statement syntax. White-listing, or only allowing required characters, is the preferred method. There are a number of online resources to assist developers in performing input sanitization. Please refer to the references below for links to these secure programming resources.

Some considerations in protecting against SQL Injection attacks:

1. Validate and escape all user provided input before passing it to the backend database.
2. Avoid using dynamic SQL whenever possible. Dynamic SQL refers to any situation in which user-supplied input is concatenated with pre-defined SQL. Stored procedures or parameterized SQL can be used as a safer alternative.
3. Apply the principle of least-privilege to web applications that interact with your database. It is a good idea to create an account for your web applications that has as few data access rights as possible to limit the scope of damage in the event that a system is compromised.
4. Turn off debugging information as it is often used to gather data for subsequent attacks.
5. Review server applications for possible SQL injection vulnerabilities, and apply all necessary code revisions and appropriate vendor patches after appropriate testing.
6. Consider implementing Web Application Firewall (WAF) technology on the web servers.
7. Consider encrypting the sensitive information in the database.

REFERENCES:

Open Web Application Security Project (OWASP)
http://www.owasp.org/index.php/SQL_injection

Web Application Security Consortium (WASC)

http://www.webappsec.org/projects/threat/classes/sql_injection.shtml

Microsoft
http://blogs.iis.net/nazim/archive/2008/04/28/filtering-sql-injection-from-classic-asp.aspx

Information Week
http://www.informationweek.com/news/security/attacks/229900111

InfoSecurity
http://www.infosecurity-us.com/view/18265/another-comodo-partner-attacked-using-sql-injection

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/